UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

7590 06/30/2006

David B Cochran
Jones Day Reavis & Pogue
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/594,368	LITTLE, HERB A.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the Applicant's Appeal Brief filed March 30, 2006.

Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn.

The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language and responses to previously presented arguments.

Claims 1-45 are pending and herein considered.

Request for Information - 35 USC §1. 105

In the course of examining or treating a matter in a pending or abandoned application filed under 35 U.S.C. **111** or **371** (including a reissue application), in a patent, or in a reexamination proceeding, the examiner or other Office employee may require the submission, from individuals identified under § **1.56(c)**, or any assignee, of such information as may be reasonably necessary to properly examine or treat the matter, for example:

(iii) *Related information*: A copy of any non-patent literature, published application, or patent (U.S. or foreign), by any of the inventors, that relates to the claimed invention.

While examining the Applicant's invention, the Examiner has come upon international applications by the Applicant not previously disclosed. The Examiner

would like to request at this time that the Applicant disclose all patents and applications for patents in the United States as well as any other foreign countries they may have filed in.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Schneier et al., US Pat 5,956,404.

Regarding **Claims 1, 16, and 31**, Schneier teaches a public-key encryption process and system comprising the steps of a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair (see Schneier col.1 lines 28-44); and b) signing a digital signature using the ephemeral key pair (see Schneier col.1 lines 45-65).

Regarding **Claims 2, 17, and 32**, Schneier teaches a public-key encryption process and system wherein the encrypting step uses an El Gamal encryption scheme (see Schneier col.1 lines 45-65).

Regarding **Claim 3**, Schneier teaches a public-key encryption process wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme; wherein the step of generating the digital signature includes hashing the plaintext message (see Schneier col.1 lines 45-65).

Regarding **Claims 18, and 33**, Schneier teaches a public-key encryption process and system wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme (see Schneier col.1 lines 45-65).

Regarding **Claims 4, 19, and 34**, Schneier teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG, where G is a generator (see Schneier col.1 lines 28-44).

Regarding **Claims 5, 20, and 35**, Schneier teaches a public-key encryption process and system for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key A = aG, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key B = bG,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A (see Schneier col.1 lines 28-44).

Regarding **Claims 6, 21, and 36**, Schneier teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG (see Schneier col.1 lines 28-44).

Regarding **Claims 7, 22, and 37**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the sender, generating a secret key K = xB and encrypting a plaintext message using the secret key K to generate a ciphertext message (see Schneier col.1 lines 28-44).

Regarding **Claims 8, 23, and 38**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature (see Schneier col.1 lines 45-65).

Regarding **Claims 9, 24 and 39**, Schneier teaches a public-key encryption process and system, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver (see Schneier col.1 lines 45-65).

Regarding **Claims 10, 25, and 40**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the receiver, generating the secret key K = bX = bxG = xbG = xB, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s (see Schneier col.1 lines 45-65).

Regarding **Claim 11**, Schneier teaches a the public-key encryption process of Claim 1, wherein at least a two-stage public-key encryption process is used; wherein the first stage includes key establishment and the second stage includes encryption/decryption; wherein said steps (a) and (b) are performed during the second stage of encryption (see Schneier col.1 lines 45-65).

Regarding **Claims 12-15, 26-30 and 41-45**, Schneier teaches a public-key encryption process and system and its implementation in wireless hand-held communication devices within a communication system (see Schneier col.5 lines 8-40).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T. Teslovich
June 24, 2006

KAMBIZ ZAND
PRIMARY EXAMINER